UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/874,984	05/01/2013	Yoji KAMIKAWA	RYM-723-3738	2783

27562 7590 01/30/2017
NIXON & VANDERHYE, P.C.
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
NAGHDALI, KHALIL	

ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
01/30/2017	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTOMAIL@nixonvan.com
pair_nixon@firsttofile.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte YOJI KAMIKAWA, TAIYO HARA, MAKOTO TAKANO,
KOJIRO TAGUCHI, HIROKAZU SHIMAOKA, and YUYA ONO

Appeal 2016-002181
Application 13/874,984[1]
Technology Center 2400

Before CAROLYN D. THOMAS, JEFFREY S. SMITH, and
TERRENCE W. MCMILLIN, *Administrative Patent Judges.*

MCMILLIN, *Administrative Patent Judge.*

DECISION ON APPEAL

This is a decision on appeal under 35 U.S.C. § 134(a) from the final rejection of claims 1–18. Final Act. 1. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM-IN-PART.

[1] According to Appellants, the real party in interest is Nintendo Co., Ltd. App. Br. 3.

REJECTIONS ON APPEAL

Claims 1–18 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Abelow (US 2012/0069131 A1; published Mar. 22, 2012) and Klitsner et al. (US 2007/0155204 A1; published July 5, 2007).

THE CLAIMED INVENTION

The present invention generally relates to an information processing system, an information processing apparatus, and an information processing method, and more particularly to information processing for accessing a server or content provider. Spec. 1. Independent claim 1 is directed to a system; independent claim 9 is directed to an apparatus; independent claim 10 is directed to a non-transitory computer readable storage medium; and independent claim 11 is directed to a method. App. Br. 24–27 (Claims App'x).

Claim 1 recites:

> 1. An information processing system comprising a server which provides a specific service and an information processing apparatus including a predetermined application for receiving a provision of the specific service, wherein the information processing apparatus comprises at least one processor at least configured to:
>
> execute the predetermined application;
>
> acquire a white list from a server controlled by a provider which provides the specific service; and
>
> when content for the specific service is requested in the predetermined application, determine, in accordance with the acquired white list, whether or not it is possible to access a server which provides the requested content in the predetermined application.

ANALYSIS

Claims 1–3, 7–11, and 17

Appellants contend the combination of Abelow and "Klitsner does not disclose that the white list applied to the dongle is used to perform a determination of 'whether or not *it is possible to access a server* which provides the requested content in the predetermined application,'" as recited in claim 1. App. Br. 15 (emphasis added). In response, the Examiner finds Klitsner teaches "the dongle is a predetermined application," and "the dongle is recognized by the server . . . then a white list is presented," and determining "a particular predetermined application provide[d] a specific white list" wherein the server allows user navigation "through the set of sites." Ans. 2–3. We agree with the Examiner.

As cited by the Examiner, Klitsner discloses:

> . . . when a *dongle is recognized by the server, the server applies a white list to the electronic device coupled with the dongle*. The white list includes a *set of web sites that the electronic device is permitted to navigate*, for the time that the dongle is coupled. For instance, a dongle is configured to provide access to the Nickelodeon® web site hosted by the Disney corporation. *When the dongle for Nickelodeon access is coupled to a networked personal computer and identifies itself to the server*, through the network, *the server provides a white list to the personal computer based on the identification*. In this case, the white list comprises a *set of Nickelodeon sites selected for the dongle* such that the personal computer is permitted navigation to only sites on the white list.

Klitsner ¶ 176 (emphases added). In other words, Klitsner describes acquiring an authorized white list for a dongle coupled to a device, the white list providing a set of server accessible sites, and providing access to that white list and navigation of the white list when the dongle is recognized. As such, Klitsner teaches or suggests determining, in accordance with the white list for a coupled dongle, whether it is possible to access sites from the server based on what sites are listed on the white list provided by the server.

Appellants have not provided persuasive evidence that "determine, in accordance with the acquired white list, whether or not it is possible to access a server which provides the requested content in the predetermined application," as recited in claim 1, is not taught or otherwise suggested by Klitsner's allowed navigation through a white list based on the server provided white list for a coupled dongle.

Accordingly, we sustain the § 103(a) rejection of independent claim 1, as well as the rejection of commensurate independent claims 9–11, and the rejection of dependent claims 2, 3, 7, 8, and 17, not separately argued. *See* App. Br. 16.

Claims 4 and 5

Appellants contend the combination of Abelow and Klitsner does not teach or suggest "at least one processor is further configured to *execute a further application different from the predetermined application when* it is *determined that it is impossible to access the server which provides the content*, thereby to access the server which provides the content by the further application," as recited in claim 4. App. Br. 16–17 (emphasis added). In response, the Examiner finds Klitsner teaches using another application that is not the predetermined application. Ans. 3. We agree with the Examiner.

As cited by the Examiner, Klitsner discloses:

> The authentication procedure preferably employs the hidden information on the dongle such that its activities are

> transparent, and typically require no interaction or information from the user.
>
> After authentication proceeds at the step 1815, the process 1800 concludes. If, however, at the step 1810, *an entry for the authentication program is not located in the registry of the electronic device, then* the process 1800 transitions to the step 1820, where *a browser automatically launches with a remote location for authentication*.

Klitsner ¶¶ 155–156 (emphases added). In other words, Klitsner describes authentication for the dongle, resulting in server access and provision of a white list, by attempting authentication from one location and then authenticating instead from a different remote location when access is not possible from the first location. As such, Klitsner teaches or suggests authenticating from one location, or executing one application, determining it is impossible to authenticate and thereby to access the server from the one location, and then authenticating from a second remote location, or executing a further application different from the first application.

Appellants have not provided persuasive evidence that "execute a further application different from the predetermined application when it is determined that it is impossible to access the server which provides the content," as recited by claim 4, is not taught or otherwise suggested by Klitsner's authentication of a dongle for access to the server from a remote location when authentication is impossible from a first location.

Accordingly, we sustain the § 103(a) rejection of claim 4, as well as the rejection of claim 5, not separately argued.

Claim 6

Appellants contend the combination of Abelow and Klitsner does not teach or suggest "at least one processor is configured to suspend the performance of the predetermined application prior to the execution of the further application," as recited in claim 6. App. Br. 18. The Examiner responds Abelow teaches suspending the use of a particular device and Klitsner teaches disabling functionality. Ans. 4. Appellants argue "Abelow teaches suspending a particular device not the performance of a predetermined application," and "suspending the particular device by Abelow would not allow for execution of the further application." App. Br. 18.

We agree with Appellants. Abelow discloses "a device . . . is in use . . . and an identity or a user provides a manual command to suspend . . . said device . . . whereby 'suspend' includes saving said device's state." Abelow ¶ 819. In other words, Abelow teaches suspending *a device.*

Contrary to the Examiner's findings, Abelow merely teaches suspending a device and saving the state of a device. Suspending a device inherently suspends the application running on the device, but fails to provide for the *subsequent execution of another application*. As such, the combination of Abelow and Klitsner does not teach or suggest "at least one processor is configured to *suspend the performance* of the predetermined application *prior to the execution of the further application*," as recited in claim 6 (emphasis added).

Therefore, we do not sustain the § 103(a) rejection of claim 6.

Claim 12

Appellants contend the combination of Abelow and Klitsner does not teach or suggest "when the predetermined application is executed, send a request for the white list, the request including an electronic certificate authorizing the information processing apparatus to access the requested white list," as recited in claim 12. App. Br. 18. Specifically, Appellants argue Klitsner does not use an electronic certificate when authenticating a dongle for access to content and does not teach a request for a white list includes an electronic certificate. App. Br. 19.

Appellants' argument against Klitsner separately from Abelow does not persuasively rebut the combination made by the Examiner. One cannot show non-obviousness by attacking references individually, where the rejections are based on combinations of references. *In re Merck & Co., Inc.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986); *In re Keller*, 642 F.2d 413, 425 (CCPA 1981).

Specifically, we agree with the Examiner's finding that claim 12 only introduces an electronic certificate, "and the electronic certificate is disclosed by Abelow." Ans. 5. For example, Abelow discloses:

> The identity provider determines if the device and/or identity is authorized and provides the appropriate authentication, which may also include providing a certificate, pass key, cookie etc. for subsequent sign-ons by said device and identity.

Abelow ¶ 1656. In other words, Abelow describes determining if a device is authorized by utilizing an electronic certificate. Klitsner teaches acquiring a white list for an authorized dongle coupled to a device, the white list providing a set of server accessible sites, and providing access to that white list and navigation of the white list when the dongle is recognized. *See* Klitsner ¶ 176.

Appellants have not provided persuasive evidence that "when the predetermined application is executed, *send a request for the white list, the request including an electronic certificate* authorizing the information processing apparatus to access the requested white list," as recited in claim 12 (emphasis added), is not taught or otherwise suggested by the Klitsner's coupling of a dongle, and then authorizing the dongle in order to access a white list, combined with Abelow's authorizing of a device using an electronic certificate.

Accordingly, we sustain the § 103(a) rejection of claim 12.

Claim 13

Appellants contend the combination of Abelow and Klitsner does not teach or suggest "when it is determined that it is not possible to access the server which provides the requested content in the predetermined application, suspend operation of the predetermined application and activate another application, different from the predetermined application," as recited in claim 13. App. Br. 19–20. In response, the Examiner finds Klitsner teaches using another application that is not the predetermined application. Ans. 3; *see* Ans. 5. The Examiner further finds Abelow teaches suspending the use of a particular device. Ans. 4. We agree with the Examiner.

As cited by the Examiner, Klitsner teaches authenticating the dongle from one location, determining it is impossible to authenticate and thereby to access the server from the one location, and then authenticating from a second remote location. *See* Klitsner ¶ 156. Abelow teaches suspending a device, which includes suspending the applications on the device as it suspends the device state. *See* Abelow ¶ 819.

Appellants have not provided persuasive evidence that: "when it is determined that it is not possible to access the server which provides the requested content in the predetermined application," as recited in claim 13, is not taught or otherwise suggested by Klitsner's determining it is impossible to authenticate from one location; "suspend operation of the predetermined application," as recited in claim 13, is not taught or otherwise suggested by Abelow's suspending device state; and "activate another application, different from the predetermined application," as recited in claim 13, is not taught or otherwise suggested by Klitsner's authenticating from a second remote location when it is impossible to authenticate from a first location.

Accordingly, we sustain the § 103(a) rejection of claim 13.

Claims 14–16 and 18

Appellants contend the combination of Abelow and Klitsner does not teach or suggest "when the other application is activated, the other application sends a request for the requested content to the server which provides the requested content, and the other application receives the requested content," as recited in claim 14. App. Br. 20–21. The Examiner responds that Klitsner "discloses where the other application after authentication through a remote location will have access to content." Ans. 5. Appellants argue that Klitsner's automatically launched application "is launched for authentication of the electronic device" but does not send "a request for the requested content to a server which provides the requested content." App. Br. 21.

We agree with Appellants. Klitsner teaches acquiring a white list for a dongle coupled to a device, the white list providing a set of server accessible sites, and providing access to that white list and navigation of the white list when the dongle is recognized. *See* Klitsner ¶ 176. Separately, Klitsner teaches authenticating the dongle from one location, determining it is impossible to authenticate and thereby to access the server from the one location, and then authenticating from a second remote location. *See* Klitsner ¶ 156.

Contrary to the Examiner's findings, while Klitsner teaches providing access to a server and sites in accordance with a server provided white list for a dongle, Klitsner's use of a remote location when it is impossible to authenticate the dongle from a first location merely teaches a method *for authenticating* the dongle. However, Klitsner's remote location only provides authentication and does not include requesting the requested content from the server. As such, the combination of Abelow and Klitsner does not teach or suggest "when the other application is activated, *the other application sends a request for the requested content to the server which provides the requested content,* and the *other application receives the requested content*," as recited in claim 14 (emphasis added).

Therefore, we do not sustain the § 103(a) rejection of claim 14. Claim 18 contains limitations commensurate to those of claim 14, and claims 15 and 16 are dependent on claim 14. We do not sustain the rejection of claims 15, 16, and 18 for the reasons stated above with regard to claim 14.

CONCLUSION

The rejection of claims 1–5, 7–13, and 17 is affirmed.

The rejection of claims 6, 14–16, and 18 is reversed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED-IN-PART